## ECS Configuration Change Request

Page 1 of 1 Page(s)

| | | | | | | |
|---|---|---|---|---|---|---|
| 1. Originator<br>Henry Baez | 2. Log Date:<br>00 - 0941 | 3. CCR #:<br>00-0941 | 4. Rev:<br>- | 5. Tel:<br>301-925-1025 | 6. Rm #:<br>2101D | 7. Dept.<br>SED |

8. CCR Title: Install and run Distributed Denial of Service trojan detection tool on baseline Solaris systems in the VATC.

| | | | |
|---|---|---|---|
| 9. Originator Signature/Date<br>9-8-2000 | 10. Class<br>II | 11. Type:<br>CCR | 12. Need Date: 9/~~00~~/2000<br>25 |

| | | |
|---|---|---|
| 13. Office Manager Signature/Date<br>9/8/00 | 14. Category of Change:<br>Initial ECS Baseline Doc. | 15. Priority: (If "Emergency" fill in Block 28).<br>Routine |

| | | |
|---|---|---|
| 16. Documentation/Drawings Impacted:<br>910-TDA-003 | 17. Schedule Impact: | 18. CI(s) Affected: |

| | | |
|---|---|---|
| 19. Release Affected by this Change:<br>~~5A~~ 5B, 6A | 20. Date due to Customer: | 21. Estimated Cost:<br>None - Under 100K |

22. Source Reference: □NCR (attach) □Action Item □Tech Ref. □GSFC □Other:

23. Problem: (use additional Sheets if necessary)
The National Infrastructure Protection Center has developed a tool to check Solaris systems for most of the major Distributed Denial of Service (DDOS) tools found in the wild. DDOS attacks uses a number of systems to attack a network and saturated that network with so much traffic that the network is rendered un-useable. The attackers compromise systems at many locations and install trojan tools with out the knowledge of the owners of those systems. CERT, NASIRC, and other security organizations highly recommend that this software be run on all networked Solaris systems to detect the presents of the DDOS trojan.

24. Proposed Solution: (use additional sheets if necessary)
Request permission to load and run the executable, FIND_DDOS version 3.3, on baseline Solaris 2.5.1 platforms in VATC on a non-interference basics to verity that there is no danger in releasing the software to the DAACs. Further, we request and recommend that the executable be put in a root-only automounted directoy for ease of execution then removed as soon as the test is completed.
FIND_DDOS_V33_SPARC.TAR CKSUM ~~[illegible] 476[illegible] 207~~ 806418831 105984
This tool has been tested in the IDG Test Cell and all Functionality Lab machines with w/o problems.

25. Alternate Solution: (use additional sheets if necessary)
The outside or perimeter of ECS networks could be strengthen with firewalls that would offer protection to all the platforms.

26. Consequences if Change(s) are not approved: (use additional sheets if necessary)
ECS runs the risk that intruders will use ECS compromise systems to attack other network and generating so much traffic that not only the attacked network but also the ECS network is affected. This happened to several university systems in California in February.

27. Justification for Emergency (If Block 15 is "Emergency"):

28. Site(s) Affected: □EDF □PVC ☒VATC □EDC □GSFC □LaRC □NSIDC □SMC □AK □JPL □EOC □IDG Test Cell □Other

| | | |
|---|---|---|
| 29. Board Comments: | 30. Work Assigned To: | 31. CCR Closed Date: |

| | |
|---|---|
| 32. EDF/SCDV CCB Chair (Sign/Date): 9/25/00<br>9/25/00 | Disposition: [✓ Approved] App/Com. Disapproved Withdraw Fwd/ESDIS ERB |
| 33. M&O CCB Chair (Sign/Date): | Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS |
| 34. ECS CCB Chair (Sign/Date): | Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB |

ORIGINAL